UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/735,509	12/12/2003	Sudarshan Palliyil	JP920030270US1	5856

39903 7590 03/13/2008

IBM ENDICOTT (ANTHONY ENGLAND)
LAW OFFICE OF ANTHONY ENGLAND
PO Box 5307
AUSTIN, TX 78763-5307

EXAMINER	
TURCHEN, JAMES R	

ART UNIT	PAPER NUMBER
2139	

MAIL DATE	DELIVERY MODE
03/13/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/735,509	PALLIYIL ET AL.	
	Examiner	Art Unit	
	JAMES TURCHEN	2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *24-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *24-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 24-44 are pending. Claims 24, 31 and 38 are amended.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/17/2008 has been entered.

Response to Arguments

Applicant's arguments with respect to claims 24, 31, and 38 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 24-29, 31-36 and 38-43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti (US 7,143,113) in view of Szor (US 2005/0022018).

Regarding claim 24:

Radatti discloses a method comprising the steps of:

computing first hash values derived from and representing a plurality of replicas of a resource, wherein the replicas are stored on respective data processing systems within a network [*column 3 lines 17-34, the baseline is formed from the master system, all of the subsequent systems are replicas of the master system; therefore hash values derived from a master system represent a plurality of replicas*];

a) storing the computed first hash values [*column 3 lines 44-48, the secure system data is retained in a storage area, either internally or externally*];

b) computing current hash values for the replicas of the resource [*column 5 lines 28-34, in the comparison cycle, files are taken one at a time and hashed (MD5)*];

c) comparing the current and first hash values in order to identify whether all the hash values match, wherein nonmatching first and current hash values for a respective one of the replicas indicates the respective one of the replica has changed since the computing of the first hash value [*column 5 lines 33-58, the recent hash is compared with the old hash*];

d) detecting that a vulnerability exists responsive to the hash value comparison indicating more than a predetermined number of changed replicas of the resource, and that no vulnerability exists responsive to the hash value comparison indicating less than or equal to the predetermined number of changed replicas [*column 7 lines 54-58, if an unauthorized user changes the contents, the files modified by the virus will differ*]; and

e) presenting a message for a user indicating a vulnerability, wherein the presenting is responsive to the predetermined number being exceeded [*column 7 lines*

24-28, reporting may be used; as is well known in the art it is inherent that the reporting will take place after detection].

Radatti does not disclose wherein the predetermined number is at least one. Szor is similar to Radatti in that Szor provides a method for network intrusion detection. Szor discloses a local analysis center (LAC) that receives notification packets about malicious code [*paragraphs 102-104*]. The LAC then checks to see if an attack threshold has been exceeded which is incremented by one for each notification packet [*paragraphs 108-109*] then appropriate action is taken [*paragraph 113*]. It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Radatti to include the functionality of the LAC of Szor in order to determine a minimum level of suspicious activity [*paragraph 108*].

Regarding claim 25:

Radatti and Szor disclose the method of claim 24, wherein steps a), b), c), and d) are performed at a first data processing system within the network [Radatti, *column 3 lines 26-34, the secure system state and secure system data file are generated on the master system; column 6 lines 11-16, the client comparison may take place internally or externally; Radatti also discloses (column 3 lines 8-16) putting an individual computer in "lock down" and scanning for a baseline (in this case a, b, c, and d are performed inside a single computer)*].

Regarding claim 26:

Radatti and Szor disclose the method of claim 24, wherein step b) is performed at each replica's respective data processing system, the method further comprising

sending the computed hash values to a first data processing system [Radatti, *column 6 lines 11-16, the hash values can be sent to an external processing system*].

Regarding claim 27:

Radatti and Szor disclose the method of claim 24, wherein the vulnerability includes a vulnerability to a computer virus [Radatti, *column 6 lines 17-38, compared against hashes of viruses*].

Regarding claim 28:

Radatti and Szor disclose the method of claim 24, wherein the vulnerability includes a vulnerability to computer hacking [Radatti, *column 6 lines 17-38, compared against hashes of Trojans and back doors*].

Regarding claim 29:

Radatti and Szor disclose the method of claim 24 further comprising:

classifying as vulnerable the data processing systems storing the replicas, wherein the classifying is responsive to the predetermined number or changed replicas of the resource being exceeded [Radatti, *column 9 lines 26-44, dangerous hash values are stored in the dangerous hash value data file, the comparison cycle will then compare new hashes with the dangerous hash file*].

Regarding claims 31-36 and 38-43:

Claims 31-36 and 38-43 are the system and computer program product corresponding to the method claims 24-29 and are rejected under the same reasoning.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 30, 37, and 44 are rejected under 35 U.S.C. 103(a) as being unpatentable over Radatti and Szor as applied to claims 24, 31, and 38 above, and further in view of A Distributed Approach against Computer Viruses Inspired by the Immune System hereafter Immune System.

Radatti and Szor disclose the method of claim 24, the steps further comprising:

selecting a sequence of vulnerability-resolution instructions relevant to the vulnerability [Radatti, *column 7 lines 59-65, the infected files may be restored to a known good state*].

Radatti and Szor do not disclose sending a notification of the vulnerability to each data processing system storing one of the replicas and sending the selected instructions to each of the data processing systems storing one of the replicas. Immune System teaches sending a notification of infection to other computers on the LAN to inform them of possible computer viruses (Page 912 – Section 3.3). Each computer in the LAN is programmed to scan its own file upon receiving notification of infection from another computer (Page 912 – Section 3.3). It would have been obvious to one of ordinary skill in the art at the time of invention to modify the method of Radatti and Szor with the notification system of Immune System in order to notify the other computers in the

network (Section 3.3.). Radatti, Szor or Immune System do not disclose sending selected instructions to each of the data processing systems storing one of the replicas, however, Radatti and Immune system are pre-programmed to handle the situation in which a notification of virus infection has occurred on another computer, then the two will scan their own files to ensure they are virus free. Sending instructions to a computer is well known in the art (JAVA, distributed processing systems, remote access and various other client-server models) and it would have been obvious to one of ordinary skill in the art to allow instructions to be received via the network instead of being pre-programmed in order to facilitate a more flexible reaction system to viruses and network intrusions.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES TURCHEN whose telephone number is (571)270-1378. The examiner can normally be reached on MTWRF 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kristine Kincaid can be reached on (571)272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Christian LaForgia/
Primary Examiner, Art Unit 2139

JRT